UnB | STI

Plano de Contingência da Secretaria de Tecnologia da Informação da Universidade de Brasília

Secretário de TI

Jacir Luiz Bordim

Coordenadoria de Gestão e Planejamento – CGESP

Francisco Jackson Alves de Freitas

Divisão de Contratações e Aquisições de TIC

Wellington Ferreira

Divisão de Apoio à Governança de TIC

André de Lanna Sette Fiuza Lima

Núcleo de Capacitação

Henrique de Almeida Ramos

Diretoria de Operações e Serviços - DOS

Domingos Pereira Costa

Coordenadoria de Redes e Infraestrutura

Alex Anderson Dantas Fidelis

Coordenadoria de Serviços Especializados

Marcus Vinicius da Silva Jorge

Coordenadoria de Segurança da Informação

Juvenal dos Santos Barreto

Divisão de Atendimento ao Usuário

Luís Miguel Antonio Gomes

Divisão de Data Center

Rodrigo Coelho Guidotti

Diretoria de Sistemas da Informação

Consuelo Martins Galo

Coordenadoria de Sistemas Administrativos

Leonardo Muzzi Soares

Coordenadoria de Sistemas Acadêmicos

Felipe Evangelista dos Santos

Coordenadoria de Sistemas de Pessoal

Andrei Lima Queiroz

Coordenadoria de Estratégia de Dados

Tiago Medina Chagas

Coordenadoria de Sites Corporativos

Rodrigo Siqueira Rocha

Equipe Técnica

Domingos Pereira Costa

Fernando Alecsandro dos Santos Teixeira

Juvenal dos Santos Barreto

Rodrigo Coelho Guidotti

Equipe de Apoio

André de Lanna Sette Fiuza Lima

Antônio Carlos Baptista de Oliveira

John Lenon da Silva Rodrigues

Histórico de Revisões

Data	Versão	Descrição	Autor
01/08/2022	1.0	Modelo Inicial	Equipe Técnica
02/08/2022	1.1	Revisão	Antônio Carlos, André de Lanna, Jacir Bordim, Francisco Jackson, Rodrigo Guidotti, Fernando Alecsandro, Fernando de Britto, Domingos Pereira.
04/08/2022	1.2	Revisão	Jacir Bordim, Antônio Carlos, André de Lanna, Francisco Jackson, Rodrigo Guidotti, Fernando Alecsandro, Fernando de Britto, Domingos Pereira, Juvenal dos Santos Barreto, John Lenon da Silva Rodrigues.
28/07/2023	1.3	Atualização	Jacir Bordim, Antônio Carlos, André de Lanna, Francisco Jackson, Rodrigo Guidotti, Fernando Alecsandro, Domingos Pereira, Juvenal dos Santos Barreto, John Lenon da Silva Rodrigues e Camila Santana Carvalho.

Das Responsabilidades

Responsável	Secretaria de Tecnologia da Informação - STI/UnB
Aprovado por:	Jacir Luiz Bordim
Políticas / Planos Relacionadas	Plano de comunicação - monitoramento NOC. Documento restrito firmado entre STI e empresas terceirizadas
Número do SEI	23106.063800/2022-72
Data da Aprovação	01/08/2023

Sumário

Tabelas

DEFINIÇÃO E TERMOS UTILIZADOS NESTE DOCUMENTO

a) **Equipe de monitoração:** responsáveis pelo monitoramento e gestão dos incidentes relacionados aos serviços críticos de Tecnologia da Informação (TI) do Núcleo de Operação de Redes (NOC - Network Operation Center - da UnB);
b) **Ativos de TI**: são todos os componentes que compõem a infraestrutura de Tecnologia da Informação utilizados pela UnB, hardwares, softwares, redes e outras tecnologias que agregam valor ao cumprimento de sua missão.
c) **Contingência:** situação de risco com potencial de ocorrer, inerente às atividades, serviços e equipamentos, e que ocorrendo se transformará em uma situação de emergência;
d) **Equipe de Prevenção, Tratamento e Reposta a Incidente Cibernético (ETIR):** equipe responsável por agir proativamente, receber, analisar e responder às notificações e atividades relacionadas aos incidentes cibernéticos ocorridos descrevendo sua natureza, as causas, a data de ocorrência, a sua frequência e os custos resultantes;
e) **Garantia:** Período em que o produto ou serviço contará com o suporte do fornecedor para garantir a sua disponibilidade e/ou correto funcionamento.
f) **Grupo responsável:** setores da STI responsáveis por um ou mais serviços críticos;
g) **Incidente:** qualquer evento que traga indisponibilidade ou falha nos ativos de TIC;
h) **Nobreak:** dispositivo alimentado a bateria, capaz de fornecer energia elétrica ao sistema por um certo tempo em caso de interrupção de energia elétrica;
i) **Sala cofre:** ambiente estanque que visa garantir a máxima segurança ao Data Center envolvendo a proteção, seja de mídias físicas ou eletrônicas, armazenamento de dados, equipamentos ou documentos de alta importância operacional ou estratégica contra incêndios, alagamentos, calor, umidade, pó, poeira, fumaça ou qualquer outra variação ambiental brusca ou extrema que coloque em risco a continuidade dos serviços nela hospedados;
j) **Serviços críticos:** são sistemas e ativos fundamentais ao pleno funcionamento da UnB e que estão hospedados dentro do ambiente da STI.

1. INTRODUÇÃO

Este documento apresenta um plano de contingência que deve ser utilizado imediatamente após a identificação de falhas ou inconsistências nos serviços (críticos) de Tecnologia da Informação (TI) disponibilizados pela Secretaria de Tecnologia da Informação - STI para os usuários da Universidade de Brasília (UnB). Este documento define ações e métodos de comunicação a serem executados em caso de falha nos serviços considerados como críticos disponibilizados pela STI.

2. APLICAÇÃO

Este documento se aplica a todos os serviços críticos, detalhados na “Tabela 5 - Relação de serviços críticos”, suportados pela Secretaria de Tecnologia da Informação (STI) da Universidade de Brasília (UnB) fornecidos para sua comunidade.

3. CENÁRIO

3.1. Serviços de Tecnologia da Informação

A Secretaria de Tecnologia da Informação (STI) é responsável pela coordenação, padronização, supervisão, custódia das informações e acompanhamento dos recursos de tecnologia de informação e comunicação coorporativas, responsável por assegurar a confidencialidade, integridade e disponibilidade da informação por meio de adoção e aplicação de mecanismos e controles de segurança alinhados às políticas e normativos internos e externos, visando obter maior eficiência institucional nas atividades de ensino, pesquisa, extensão e gestão universitária.

Os processos de gerenciamento e gestão de serviços de Tecnologia da Informação e Comunicação (TIC) abrangem a entrega dos serviços de TIC com a finalidade de fornecer o suporte necessário aos objetivos da instituição e de atender às necessidades dos usuários, compreendendo a integração entre pessoas, processos e tecnologias que compõem a Universidade, considerando as melhores práticas de gerenciamento de TIC nas organizações adaptando alguns processos à maturidade da UnB para melhorar a qualidade e propiciar uma melhor gestão.

3.2. Infraestrutura

No ambiente gerenciado pela Secretaria de Tecnologia da Informação, responsável pela infraestrutura de TI dos serviços críticos, há uma variedade de aspectos que definem as atividades e o funcionamento do ambiente de TI.

Para manter o ambiente dentro de níveis aceitáveis de recuperação de incidentes e problemas relacionados ao funcionamento do ambiente de TI, são definidos Acordos de Nível de Serviço (ANS). O ambiente de monitoramento de serviços e sistemas do NOC da UnB opera de maneira ininterrupta. Também há o ANS referente à recuperação, englobando manutenção preventiva e corretiva do sistema de alta disponibilidade (Sala Cofre).

4. ATRIBUIÇÕES E RESPONSABILIDADES

PAPEL	RESPONSABILIDADE
Secretário de TI	• Aprovar o plano de contingência e solicitar atualizações.
Analista de monitoração	• Monitorar de forma ininterrupta o ambiente computacional de alta disponibilidade. • Acionar a direção, os chefes de área, os coordenadores e/ou grupo responsável pelo acordo com o meio de comunicação adequado. • Registrar, tratar e/ou escalonar os chamados relacionados aos eventos do sistema de monitoramento.
Grupo responsável	• Tratar e solucionar os incidentes relacionados aos serviços críticos. • Identificar oportunidades de melhorias sugerindo atualizações do plano sempre que necessário.

Tabela 1: Atribuições e responsabilidades

5. HIERARQUIZAÇÃO DE RESPONSABILIDADES PARA ATENDER OS SERVIÇOS CRÍTICOS

5.1. Equipe de monitoração

A equipe de monitoração é composta pelo NOC da UnB, atua de forma reativa, preventiva e proativa com objetivo de manter o ambiente de TI o mais estável possível e quando identificam algum alerta que não consigam resolver acionam o Grupo Responsável.

5.2. Grupo responsável

Os coordenadores serão comunicados sempre que um serviço crítico estiver com algum evento do sistema de monitoramento.

Listagem dos setores responsáveis pela execução das atividades.

GRUPO RESPONSÁVEL	E-MAIL
Coordenação de Redes e Infraestrutura (DOS/CRI)	sti.cri@unb.br
Coordenação de Estratégia de Dados (DSI/CED)	sti.ced.unb.br
Coordenação de Segurança da informação (DOS/CSI)	sti.csi@unb.br
Coordenação de Serviços Especializados (DOS/CSE)	sti.cse@unb.br
Divisão de Data Center (DOS/DDC)	sti.ddc@unb.br
Coordenadoria de Sites Corporativos (DSI/Sites)	sti.sites@unb.br
Coordenadoria de Sistemas Administrativos (DSI/ADM)	sti.admin@unb.br
Coordenadoria de Sistemas Acadêmicos (DSI/ACAD)	sti.acad@unb.br

Tabela 2: Grupos responsáveis

5.3. Diretorias

Os Diretores das áreas serão comunicados quando houver indisponibilidade de qualquer serviço crítico da instituição que envolva seus grupos responsáveis.

DIRETORIA	E-MAIL
Diretoria de Sistemas da Informação (DSI)	sti.dsi@unb.br
Diretoria de Operações e Serviços (DOS)	sti.dos@unb.br

Tabela 3: Diretorias das áreas

5.4. Secretário de Tecnologia da Informação

O secretário da STI será comunicado sempre que um serviço crítico estiver em risco de sofrer uma interrupção no seu funcionamento.

FUNÇÃO	E-MAIL
Secretário de Tecnologia da Informação	sti.dir@unb.br

Tabela 4: Secretaria

6. RELAÇÃO DE SERVIÇOS CRÍTICOS

Relação dos serviços essenciais ao atendimento das necessidades institucionais e funcionamento dos serviços de TIC.

SERVIÇO DE TIC	DESCRIÇÃO	GRUPO RESPONSÁVEL
Active Directory	Serviços de diretórios para computadores tombados pela Fundação Universidade de Brasília	CSE
Banco de dados	Serviços que visam proporcionar a disponibilidade, confiabilidade, integridade e guarda dos Bancos de Dados sob custódia da Secretaria de Tecnologia da Informação (STI)	CED
ServiçosTIC	Sistema de aberturas de chamados utilizado no suporte aos docentes, técnicos administrativos, discentes e prestadores de serviços.	CSE
DNS	Sistema de nomes de domínio hierárquico e distribuído de gestão de nomes para computadores, serviços ou máquinas conectadas à internet.	CSE
Internet	Gestão do acesso à rede mundial de computadores.	DDC e CRI
Portais UnB	Sites públicos da UnB com informações relacionadas ao Ensino, Pesquisa e Extensão e Gestão universitária.	Sites
Controle de acesso ao Restaurante Universitário (RU)	Sistema de acesso ao Restaurante Universitário (Catraca).	ADM
E-mail e listas de discussão	Sistema de e-mail e listas de discussão para comunidade.	CSE
SEI	Sistema de gestão dos processos e documentos eletrônicos da UnB.	DSI e CSE
SIG UnB	Sistema de administração, acadêmico e de Pessoal da UnB	ADMIN, ACAD e CSE
Rede sem fio	Serviço de fornecimento de conexão sem fio à internet para alunos, professores e servidores (UnB Wireless e Eduroam).	CRI

Tabela 5: Relação de serviços críticos

7. PRINCIPAIS RISCOS E CONTINGENCIAMENTO

Esse plano tem como objetivo ser acionado quando algum risco afetar diretamente no funcionamento dos serviços críticos, impactando na continuidade das atividades da instituição.

Com isso, a tabela abaixo mostra os principais riscos que possam impactar na continuidade dos serviços críticos listados anteriormente.

RISCO	DESCRIÇÃO	CONTINGENCIAMENTO
Acesso indevido à Sala Cofre	Acesso de pessoas não autorizadas ao ambiente interno da sala cofre.	Manter o monitoramento ininterrupto e controle de acesso da sala cofre.
Ataques Externos	Ataque cibernético que causa danos ou roubo de informação dos serviços disponíveis externamente, grande parte dos ataques são de negação do serviço, que tem como foco deixar o serviço indisponível.	Gerenciar eventos e a redundância de equipamentos de segurança de TI. Ações dos grupos responsáveis e da equipe ETIR.

RISCO	DESCRIÇÃO	CONTINGENCIAMENTO
Ataques Internos	Causados por usuários legítimos da rede, porém, tentando acessar algum serviço ou equipamento para deixá-lo indisponível.	Gerenciar eventos e redundância de equipamentos de segurança de TI. Ações dos grupos responsáveis e da equipe ETIR.
Falha Humana Acidental/Imperícia	Causada por falta de atenção, capacidade técnica ou conhecimento suficiente para dar suporte em alguns equipamentos ou sistemas.	Disponibilizar privilégio mínimo para as permissões de usuários, senhas fortes, capacitação e etc.
Falta de energia elétrica	Causada por fator externo ou interno à rede elétrica do prédio ou de sua localidade.	Utilizar o Grupo Gerador composto de um Gerador e nobreak.
Migração e Mudanças em Aplicações Virtuais	Causada na manipulação e instalação de atualizações que possam impactar nas disponibilidades dos serviços de TIC.	Controlar processo de gerenciamento de mudança.
Problema com Equipamentos (Hardwares que dão suporte aos serviços críticos)	Causado por equipamentos que por algum motivo necessitem de reparos.	Manter contratos de garantia/suporte e/ou mecanismos de redundância.
Problemas de conexão (rede interna à UnB e externa)	Causados principalmente por rompimentos de cabos de rede e fibra óptica ou por problemas em equipamentos de redes e segurança da informação.	Manter contratos de garantia/suporte e/ou mecanismos de redundância.
Falha na Identificação de Eventos	Causado por falta de pessoal para monitoramento dos eventos no serviço de monitoramento.	Firmar contrato com empresa para trabalho no Núcleo de Operação e Controle (NOC).
Indisponibilidade da Sala Cofre	Incidentes que podem comprometer a disponibilidade e/ou a integridade dos equipamentos.	Manter contrato de manutenção e a certificação da sala cofre.

Tabela 6: Principais riscos e contingenciamento

8. PLANO DE COMUNICAÇÃO

Existe um plano de comunicação interno da STI, disponibilizado para execução pela empresa terceirizada, que é colocado em prática em conjunto com este plano de contingência.

Quem deve comunicar:

Equipe de Monitoração ou qualquer servidor que detecte algum incidente que possa gerar risco aos serviços.

A quem comunicar:

Aos grupos responsáveis constantes na Tabela 2.

Como comunicar:

A comunicação será realizada por meio de e-mails, de acordo com os grupos constantes na tabela 2, e por telefonemas, conforme especificado no plano de comunicação interno.

9. CONSIDERAÇÃO FINAL

Este documento será publicado no site institucional da STI/UnB (https://sti.unb.br/), entrando em vigor a partir da data de sua aprovação. Será revisado e atualizado sempre que houver mudanças significativas na infraestrutura.